

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/513,065	02/24/2000	Chi-Pei Michael Hsing	ST9-99-167	5699

7590 08/25/2004

SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3213

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/513,065

Applicant(s)

HSING ET AL.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 May 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7,9-19,21-31 and 33-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7,9-19,21-31 and 33-43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 February 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7, 9-19, 21-31, 33-43 have been examined. Applicant has amended claims 1, 5, 9-13, 17, 21-25, 29 and 33-36; canceled claims 8, 20 and 32; and added new claims 37-43.

Response to Argument

2. The following is a response to Applicant's argument on pages 13-18 filed on May 25, 2004.

3. Applicant's arguments, see page 15, last paragraph-page 16, first paragraph, with respect to the rejection(s) of claim(s) 12, 24 and 36 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Fuh U.S. Patent No. 6,463,474.

4. Applicant's arguments with respect to claims 1-7, 9-11, 13-19, 21-23, 25-31, 33-35 and 37-43 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 29 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claim 29 recites the limitation "the server user identifier and server password". There is insufficient antecedent basis for this limitation in the claim: no server password is defined prior to the recitation of this limitation.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-7, 9-11, 13-19, 21-23, 25-31, 33-35 and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings) in view of Bryant "Designing an Authentication System: a Dialogue in Four Scenes" (hereinafter Bryant), Schneier Applied Cryptography (hereinafter Schneier) and Sokal et al. U.S. Patent No. 5,953,504 (hereinafter Sokal).

Art Unit: 2132

10. As per claims 1, 5, 6 and 9, Stallings discloses a simple authentication dialogue that uses a central authentication server to log a client onto a network of distributed services. See Stallings, page 326, 'A Simple Authentication Dialogue'. This simple authentication dialogue uses a centralized server to securely identify users by obtaining information from the user; generate a ticket with the obtained user information; and then send a ticket back to the user, which comprises of an encrypted message containing the identification of the client, the network address of the client, and the identifier of the service. This generated ticket, in addition to an identifier of the client, is sent to the service, whereupon, the service decrypts the ticket and compares the identification with the parsed identification. Since only the authentication server and the service share the private encrypted key, only the authentication server could have encrypted the ticket when issued to the client. Hence, if the parsed id matches the id sent by the client, then the request is accepted. See Stallings, page 326, steps 1, 2, and 3.

11. Stallings does not explicitly disclose the ticket contains both a username and a computer identifier to authenticate a parsed username and parsed computer identifier. However, other disclosures about the Kerberos system that detail the rationale behind the makeup of the issued tickets teach using a computer identifier in addition to the username. Bryant teaches the step of including a workstation address in the ticket issued by the Kerberos authentication method to prevent an unscrupulous workstation from intercepting an issued ticket to a valid workstation and using the ticket to access the service

Art Unit: 2132

under the guise of the valid workstation. See Bryant, page 5, especially 8th paragraph "Athena". It would be obvious to one of ordinary skill in the art at the time the invention was made, for the identity of a user during a session to comprise a username and a computer identification as taught by Bryant in the simple authentication dialogue as taught by Stallings. Motivation for such a combination would enable the invention to prevent identity duplicity by ascertaining a user by a unique name and a computer identifier. As such, the invention covered by Stallings comprises the following steps of:

- a. generating an authentication key based on a user name and a computer identifier (see Stallings, page, 326, 3rd paragraph, sentence beginning with "To do so ..."; wherein the user name is the user id and the computer identifier is the workstation address);
- b. receiving an authentication key, a user name, and a computer identifier (see Stallings, page 326, 3rd paragraph, step 3 as modified by Bryant, page 5, especially 8th paragraph "Athena:."; wherein the authentication key is effectively the Ticket);
- c. parsing the authentication key to obtain a parsed user name and computer identifier (see Stallings page 326, 4th paragraph; 2nd sentence; definition of "Ticket");
- d. validating the received user name and computer identifier using the parsed user name and computer identifier (see Stallings, page 326 2nd sentence as modified by Bryant, page 5, especially 8th paragraph "Athena:").

12. Further, Stallings does not expressly disclose the authentication key including a server user identifier. Schneier teaches a feature of securely including within an authentication key a secret. Schneier teaches securing secrets using knowledge by the recipients of the secured secrets, wherein recipients only having this knowledge can access the secrets. See Schneier, pages 70-72, sections 3.6 and 3.7, Secret Splitting and Secret Sharing. Further, a server user identifier and corresponding password are effectively secrets to be secured by a user, wherein the user uses the secret to access services. For example, Sokal discloses a server user identifier and correspond password as such a secret. See Sokal, col. 5, lines 54-57. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication key to include a server user identifier. Motivation for such a combination enables secrets to be secured and accessed only by authorized users and for the user to use the secret to obtain the services of a server. See Schneier, page 71, 6th paragraph; see Sokal, col. 5, lines 55-57. Finally, the invention covered above defines the following limitations: the generation of an authentication key comprising a client user name, a client computer identifier, the server user identifier, and a server password (see Stallings, Bryant and Schneier, *Ibid*); the server user identifier and corresponding password is obtained by parsing the authentication key (see Schneier, page 70, steps 2 and 4, XOR operation to secure and retrieve secret); and the server user identifier and corresponding password enables the client to log into the server (see Stallings, page 326, step 3). The aforementioned cover claims 1, 5, 6 and 9.

13. As per claim 2, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the validating step comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier (see Stallings, page 326, step 3; final paragraph).

14. As per claim 3, Stallings covers a method as outlined above in the claim 2 rejection under 35 U.S.C. 103(a). In addition, a match indicates that the received user name and computer identifier are valid (see Stallings, page 326, step 3; constitution of 'Ticket'; final paragraph).

15. As per claim 4, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the method further comprises, before parsing, decrypting the authentication key (see Stallings, page 326, final paragraph).

16. As per claim 7, Stallings covers a method as outlined above in the claim 6 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose that a plurality of users share a server user identifier and corresponding password. However, the use of a shared user identity to logon to a service is notoriously well known in the art. Shared user identities include a range of roles, which cover everything from a default user or guest user for restricted access, to an

Art Unit: 2132

administrator or root user for privileged access. These types of shared roles are found in popular OS server systems ranging from UNIX to Windows NT.

Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for a plurality of users to share a server user identifier and corresponding password. Motivation for such an implementation enables a simple means to classify user access.

17. As per claim 10, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). In addition, the method further comprises encrypting the authentication key (see Stallings, page 326, third paragraph).

18. As per claim 11, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). In addition, the method further comprises forwarding the authentication key to a user (see Stallings, page 326, third paragraph).

19. As per claims 13-19 and 21-23, they are apparatus claims corresponding to claims 1-7 and 9-11, and they do not teach or define above the information claimed in claims 1-7 and 9-11. Therefore, claims 13-19 and 21-23 are rejected under Stallings in view of Bryant, Schneier and Sokal for the same reasons set forth in the rejections of claims 1-7 and 9-11.

Art Unit: 2132

20. As per claims 25-31 and 33-35, they are article of manufacture claims corresponding to claims 1-7 and 9-11, and they do not teach or define above the information claimed in claims 1-7 and 9-11. Therefore, claims 25-31 and 33-35 are rejected under Stallings in view of Bryant, Schneier and Sokal for the same reasons set forth in the rejections of claims 1-7 and 9-11.

21. As per claim 41, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose that the authentication key comprises the computer identifier split into portions and the portions being interposed between the user name, the server user identifier and the server password prior to encryption. However, this feature is a typical result after a permutation step of the recited parts in a method to prepare data as taught by Schneier. See Schneier, page 271, 'The Initial Permutation' of a DES scheme. It would be obvious to one of ordinary skill in the art at the time the invention was made to permute the contents of the authentication key prior to encryption to augment the encryption process. See Schneier, page 271, 2nd paragraph, second sentence. The aforementioned covers claim 41.

22. As per claim 42, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). As mentioned above, the computer identifier is identified as a workstation address, but does not specify in greater detail that the workstation address is an IP address. However, TCP/IP is the de facto standard protocol to route messages between network devices. As such, an IP

Art Unit: 2132

address is an obvious workstation address. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the computer identifier to be identified as an IP address since it would enable unique identification of computers networked by TCP/IP as known to one of ordinary skill in the art.

23. As per claim 43, it is a method claim corresponding to claims 1-7 and 9-11 and it does not teach or define above the information claimed in claims 1-7 and 9-11. Therefore, claim 43 is rejected under Stallings in view of Bryant, Schneier and Sokal for the same reasons set forth in the rejections of claims 1-7 and 9-11.

24. Claims 12, 24 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bryant, Schneier and Sokal, and further in view of Fuh et al. U.S. Patent No. 6,463,474 (hereinafter Fuh).

25. As per claim 12, Stallings covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose intercepting the transmitted authentication key from the client to the server by the computer. However, means to intercept authentication information is a well-known feature of proxy firewalls or authentication routers, which are typically implemented as gate-keepers to a secured network and/or service: incoming requests to the secure network and/or service are submitted to the secure network and/or service but authorization is processed by the proxy device

Art Unit: 2132

unbeknownst to the requesting client. For example, Fuh teaches such an authentication proxy. See Fuh, col. 7, line 62-col. 8, line 8. It would be obvious to one of ordinary skill in the art at the time the invention was made for the computer to be an authentication proxy that intercepts a client's request to access a server. Motivation for such a combination enables the secure system to hide organization of the features from those outside the secured system. See Fuh, col. 2, lines 29-32. The aforementioned covers claim 12.

26. As per claims 24 and 36 they are claims corresponding to claims 1-7, 12, 13 and 25, and they do not teach or define above the information claimed in claims 1-7, 12, 13 and 25. Therefore, claims 24 and 36 are rejected under Stallings in view of Bryant, Schneier, Sokal and Fuh for the same reasons set forth in the rejections of claims 1-7, 12, 13 and 25.

27. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bryant, Schneier and Sokal, and further in view of VeriSign "Certification Practice Statement" (hereinafter VeriSign).

28. As per claim 37, Stallings covers a method as outlined above in the claim 9 rejection under 35 U.S.C. 103(a). Stallings does not expressly disclose emailing the authentication key to the user. VeriSign teaches emailing certified keys to clients. See VeriSign, Section 4.2, 'Method of Communicating Application' for class 1-4. It would be obvious to one of ordinary skill in the art for

Art Unit: 2132

the generated authentication key to be emailed to the user since email provides a private means to securely communicate information as known to one of ordinary skill in the art. The aforementioned covers claim 37.

29. As per claims 38, 39 and 40, they are method claims corresponding to claims 1-7, 9-11, 36 and 37, and they do not teach or define above the information claimed in claims 1-7, 9-11, 36 and 37. Therefore, claims 38, 39 and 40 are rejected under Stallings in view of Bryant, Schneier, Sokal, Fuh, and VeriSign for the same reasons set forth in the rejections of claims 1-7, 9-11, 36 and 37.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

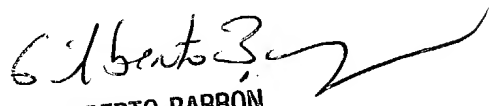
Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
August 10, 2004



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100